Offera Kubii Raspberry Pi 3 Modello B 1 GB

Il nuovo Raspberry PI 3 Modello B da 1 GB con connessioni wireless Bluetooth e WiFi integrate è disponibile ad un prezzo ridotto sul sito e-commerce di Kubii a soli € 39.90.

Basato sul processore **Quad Core Broadcom 2837ARMv8 64bit** che passa da 900 MHz (sul Raspberry Pi 2) a 1.2GHz, questo Raspberry Pi di nuova generazione è un po' più grande del Pi2, più veloce e più potente rispetto ai suoi predecessori.

Specifiche tecniche:

- Processore Broadcom 2837 Quad-Core ARMv8 64bit
- Velocità di clock: 1,2 GHz
- 1 GB di RAM
- BCM43143 WiFi integrato
- Bluetooth Low Energy (BLE) integrato
- GPIO esteso 40-pin
- 4x porte USB2
- Uscita video e stereo
- Porta CSI ìper collegare la fotocamera Raspberry Pi
- Porta DSI per collegare il touchscreen Raspberry Pi
- Lettore di schede microSD per caricare il sistema operativo e memorizzare i dati
- Alimentazione: micro-USB, ora supporta fino a 2.5A

Con il Raspberry PI 3 è possibile realizzare tanti progetti IoT, oltre che avere un piccolo pc Linux per casa e ufficio.

Cometdocs lancia una nuova versione di PDF to Word Converter

Cometdocs, un noto sistema di gestione dei documenti online, ha appena rilasciato una nuova versione di PDF to Word Converter, una delle applicazioni più apprezzate e scaricate. Quindi, non meniamo il can per l'aia e scopriamo invece che cosa ha questa versione 4.1 da offrirci.

Nuove caratteristiche

Ascoltando i feedback degli utenti, Cometdocs ha sviluppato nuove funzionalità pratiche, accompagnate dalle già note caratteristiche che vale la pena mantenere.

- Da ora in poi è possibile convertire i PDF da iCloud
- I servizi collegati sono ora gratuiti per tutti gli utenti
- È possibile rinominare il documento convertito

Oltre a queste nuove funzionalità, sono ancora disponibili le vecchie caratteristiche come il numero illimitato di conversioni, la possibilità di accedere ai file PDF da Gmail e dai servizi cloud più diffusi. Tuttavia, questo non è tutto, quindi assicuratevi di dare un'occhiata a tutte le possibilità che questa applicazione di produttività ha da offrire.

Tecnologia OCR

Anche se la tecnologia OCR delle versioni precedenti di PDF to Word Converter era soddisfacente e offriva un'ottima qualità

di conversione, gli sviluppatori di Cometdocs sono in costante ricerca della perfezione e dei miglioramenti. Pertanto, la versione più recente porta i server aggiornati e migliorati che rendono le conversioni impeccabili. In altre parole, sarete in grado di convertire file complessi e scansionati senza difficoltà.

Interfaccia utente migliorata

Le nuove funzionalità dell'interfaccia utente meritano una menzione. Così, l'UI ha avuto dei lievi cambiamenti. Mantiene ancora il design semplice e minimalista adatto a tutti i tipi di utenti, ma è ancora migliorato: un po' di lucidatura lo rende più stabile e ottimizzato.

L'unica cosa rimasta da fare è aprire App Store, cercare PDF to Word Converter e scaricarla. Non vediamo l'ora di sentire le vostre impressioni, pertanto vi preghiamo di condividerle nei commenti.

Come utilizzare il modulo ESP8266 per comodare Arduino da Smartphone

L'ESP8266 è un ottimo dispositivo hardware, che permette di aggiungere a qualsiasi prodotto, una connessione WiFi per trasferire e ricevere informazioni.

Il sistema Adapter è un adattatore che ci permette di far comunicare il nostro tablet o smarphone con il nostro progetto arduino. (link per acquisto su eBay)

Fase 1 Creazione del progetto Blynk

L'APP di riferimento è Blynk, permette di creare sul nostro dispisitivo un progetto sul quale poter posizionare Led, Bottoni Display ed altri controlli.
La prima operazione sarà quella di creare un progetto tramite Blynk e selezionare come "*Hardware Model*" ESP8266.
Al progetto verrà associato un "Auth Token" un codice alfanumerico utilizzato da blynk per associare la tua schedina Adapter al tuo progetto Appena creato, in modo sicuro.
Una vota creato il tuo progetto Blynk potrai inserire dei "*Widget*". I Widget sono dei controlli che permettono di creare la tua App, con operazioni per usare bottoni, led ecc.
Occorre copiare in memoria il Token creato dal progetto, poichè servirà in seguito per incollarlo all'interno del adapter.

Fase 2 Collegamento Adapter

Ora colleghiamo elettricamente il nostro adapter, il sistema funziona a 5v e può essere collegato direttamente alla 5V del nostro arduino, collegando quindi i pin
5V e GND. I restanti pin RX e TX dovranno essere collegati al nostro arduino in modo inverso sulla porta da noi scelta, quindi se prendiamo la porta1
di Arduino Mega, collegheremo RX1 a TX e TX1 a RX. Ora il nostro adapter è collegato e funzionante.

Fase 3 Associazione Adapter Blynk

Ora accendiamo il nostro arduino, la schedina Adapter creerà una propria rete con il nome Adapter_xxxx collegandoci a questa rete ed entrando con un
browser al indirizzo 192.168.4.1 si avàà accesso alla sua configurazione.
Entrare nella voce Blynk ed inserire il codice precedentemente copiato (preso dalla voce Auth Token) inserire il codice di sicurezza 1234 e premere save.

Tornare nella schermata precedente ed entrare nella seconda voce Wifi, selezionare la propria rete di casa, sul quale si ha l’accesso ad internet inserire la password
ed il solito codice di sicurezza (1234). Se tutto è stato scritto in modo corretto si è già pronti.

Fase 4 il protocollo (opzionale)

Blynk permette di pilotare degli ingressi fisici delle schede sul quale è installato e degli ingressi virtuali,
il protocollo di comunicazione funziona tramite gli ingressi virtuali. Ogni Widget che si inserisce nel progetto può essere un controllo di
Inputo o di Output al quale noi andremmo ad associare un ingresso virtuale da V1 a V50. Il protocollo per inviare e ricevere stringhe è molto semplice
ecco la sintassi:

Vx,Data##

dove
Vx = Rappresenta l’ingresso virtuale es V1
Data = È il campo dati che può essere una stringa
= fine comando

ecco alcuni esempi:

Scrivere Ciao su un Widget LCD associato al ingresso V10

V10,Ciao##

Ricevere l’evento della pressione di un pulsante associato al ingresso V1:

se il pulsante è premuto
V1,1##

se il pulsante non è premuto
V1,0##
Il protocollo di comunicazione è molto semplice funziona tramite una normale comunicazione seriale con un baudrate di

default di 115200bps.
Nel protocollo di comunicazione ogni messaggio che si invierà da Arduino al App Blynk avrà un ritardo di 200ms.

Fase 5

Anche se il protocollo di comunicazione è già molto semplice ed intuitivo è stata scritta una libreria per Arduino Mega e Arduino Due
(la scheda a 5 volt è compatibile a livello hardware solo con Arduino Mega), per facilitare la comunicazione con l'App senza dovere inviare o ricevere nessun messaggio, ecco un semplice esempio:

```
#include <IotDevSerLib.h>
#if defined SOFTWARE_SERIAL_OK
#include <SoftwareSerial.h> // If used Software Serial
// X Software serial #define _SS_MAX_RX_BUFF 256 // RX buffer size //BEFORE WAS 64
#define rxPin 11 // Software Serial
#define txPin 10 // Software Serial
SoftwareSerial swSer(rxPin,txPin); // If use SoftwareSerial port
#endif
IotDevSerLib IotDev;

void mngIotDev(int param, String Data)
{
switch(param)
{
case IOT_V1:
Serial.println("IOT_V1: "+Data);
if (Data.toInt()==1){
IotDev.send(IOT_V6,"Hello, World!"); //Write On Display
IotDev.send(IOT_V7,"by Adapter Iot"); //Write On Display
}
break;
case IOT_V2:
Serial.println("IOT_V2: "+Data);
if (Data.toInt()==1){
IotDev.send(IOT_V6," "); //Write On Display
```

```
IotDev.send(IOT_V7," "); //Write On Display
}
break;
default:
Serial.print("Unknow Param: ");
Serial.println(param);
break;
}
}
void setup() {
Serial.begin(115200);
IotDev.beginHW(&Serial1,115200); // Hardware Serial
//IotDev.beginSW(&swSer,115200); // Software Serial
IotDev.setCallBack(mngIotDev); //callback
Serial.println("Start");
}
void loop() {
IotDev.run();
}
```

Nello Sketch inizializziamo la porta di comunicazione ed associamo una funzione di callback per cattuarare gli eventi che arrivano dalla nostra App.
Se invece volessimo inviare qualcosa al App per comunicargli una determinata informazione dovremmo usare il metodo send (es. IotDev.send(IOT_V6,”Hello, World!”)).

Materiale

Come craccare una rete WiFi,

protetta WEP, WPA o WPA2

In questa piccola guida, vedremo come poter ottenere accesso ad una rete WiFi, protetta da password WEP, WPA oppure WPA2.

Questo articolo è stato scritto SOLO PER FINALITà CONOSCITIVE E PER TESTARE LA PROPRIA RETE. Ricorda così dice l'articolo 615.
*Chiunque **abusivamente** si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si **mantiene** contro la volontà**espressa** o **tacita** di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.*

Dopo questa piccola, ma doverosa promessa, andiamo a vedere un po' quali sono gli strumenti disponibili per poter testare una rete WiFi, contro possibili attacchi. Prima di continuare, è utile fare un po' di glossario, per poter conoscere nuovi termini:

- **SSID**: è il nome della rete, che compare quando facciamo una scansione WiFi con il nostro dispositivo
- **MAC**: è un codice che identifica un dispositivo, all'interno di una rete, meglio noto come BSSID.
- **Canale:** le reti WiFi comunicano sulle frequenze 2.4 GHz e 5 GHz e in diversi canali, che variano in base alla legislazione del paese in cui ci si trova.
- **Wardriving**: è un'attività che consiste nel mappare le reti WiFi che sono presenti in un area geografica, attraverso un dispositivo con scheda wireless e modulo GPS per la localizzazione.

Come effettuare una scansione delle reti WiFi

Uno dei primi passi per poter ottenere informazioni riguardo alla rete WiFi presenti in zona, è quello di effettuare una ricerca attraverso software. Tale operazione prende il nome di wardriving e per farla basta avere anche uno smartphone. Ci

sono diverse applicazioni disponibili sullo store, specialmente per il mondo Android, dove è possibile far lanciare questa procedura, che permette di raccogliere informazioni, come posizione GPS del router, nome della rete WiFi, tipologia di protezione, canale di trasmissione e se il WPS è attivo.

Ecco i principali tool che si utilizzano:

- Wigle Wifi Wardriving
- Kismac
- inSSIDer
- Netstumbler

I dati generati da questi software sono facilmente esportabili e analizzabili.

Reti WiFi WEP

Le reti WiFi WEP sono quelle più vecchie e dal momento che stanno diventando in disuso, sono meno frequenti durante le ricerche. L'algoritmo di cifratura dello scambio di pacchetti, durante la fase di connessione ad una rete protetta da WEP è stato bucato, nel senso che attraverso la raccolta di un determinato numero di pacchetti (tipicamente più di 10.000), è possibile scovare la password, che protegge la rete. I tool disponibili per procedere con un'attacco ad una rete WiFi protetta da WEP sono i seguenti:

- Fern WiFi Cracker
- Aircrack-NG
- Wifite

Questi software sono abbastanza semplice da poter utilizzare, in quanto dispongono di interazione guidata con l'utente e, come nel caso d Fern WiFi Cracker, una vera e propria

interfaccia grafica, che ne migliora l'usabilità. Occorre aggiungere, che un altro tipo di attacco a cui sono soggette le reti WiFi WEP, è quello della correlazione tra l'SSID e la password di default della rete. Quindi attraverso il nome della rete WiFi, che è facilmente reperibile da una scansione delle reti wireless presenti in zona, è possibile ottenere una password, che in caso non fosse stata cambiata dal proprietario della rete, permette di accedervi. Questo attacco funziona con reti WiFi di router prima del 2014, come ad esempio quelli di Alice, Telecom, Fastweb, Libero etc…, ovvero dei provider Italiani e non solo, che sono soggetti a questo tipo di attacco.

Uno dei programmi più famosi è WPA Tester disponibile per Android, che è molto semplice da usare.

Reti WiFi WPA/WPA2

Per quanto riguarda questi tipologie di reti WiFi, non esiste ancora una procedura simile a quella per le reti WEP, in quanto il meccanismo di protezione è più sofisticato rispetto a quest'ultimo. Gli attacchi possibili, riguardo il mondo del **bruteforce**, ovvero si continuano a fare tanti tentativi di password, fino a quando non si trova quella corretta. I tempi di questi attacchi, possono durare da pochi minuti ad anni, in quanto se la password è di questo tipo, si@3!£98″£NDWb123é*ff)DJIAnda, il processo è molto, ma molto lungo. L'attacco può durare meno, se si utilizzano delle liste preconfigurate, che riducano il numero di tentativi, da quasi infinito ad un numero più ridotto. Ad esempio alcune liste sono già disponibili in base al paese delle rete WiFi, dove tipicamente sono comprese le parole chiave più famose, che possono essere combinato tra di loro. Ci sono anche software, che generano delle liste di password, in base ad informazioni legate al proprietario della rete WiFi. Se ad esempio la rete WiFi è protetta da una password, che contiene il nome del cane

e il nome di battesimo del figlio del proprietario della rete, con un attacco di questo genere, è possibile risparmiare molto, ma molto tempo.

I software più importanti per le reti wireless protette da WPA/WPA2 sono:

- AirCrack-NG
- Fern WiFi cracker
- CoWPatty

Come nel caso delle reti WEP, con password **generata** dal valore **dell'SSID**, un tool come WPA Tester può verificare se la password di default è stata cambiato oppure no, anche per le reti WPA/WPA2.

C'è anche un nuovo tipo d'attacco, che non si basa tanto sulla tecnologia di protezione della rete, più che altro da un'azione fatta dall'utente, che prende il nome di attacco **phishing.** Il tool in questione si chiama wifiphisher (link) e l'attacco si basa sulla seguente dinamica;

1. La vittima, che è già connessa alla rete WiFi in questione, viene de-autenticata, attraverso espedienti hardware come jammer, oppure software
2. Il dispositivo della vittima a questo punto tenterà di connettersi ad una rete WiFi diversa dall'originale, che però ha lo stesso SSID e una potenza maggiore
3. Una volta connessa a questa nuova rete, la vittima verrà re-indirizzata in una pagina web di configurazione, dove per qualche motivo tecnico, dovrà re-inserire la password del WiFi originale
4. A questo punto il PC attaccante, avrà a disposizione la password, per poter accedere alla rete WiFi originale

Questa tipologia d'attacco è molto potente, ma richiede un'azione da parte dell'utente e qualora si dovesse

insospettire di qualcosa, potrebbe in poche minuti trovarvi fisicamente, in quanto l'attacco funziona bene quando l'attaccante si trova in prossimità dalla vittima.

Reti WIFI con tecnologia WPS

La tecnologia WPS è molto comoda, in quanto permette ad un dispositivo ed un router, di scambiarsi una chiave, sfruttando la possibilità di poter accedere fisicamente al router, premendo un pulsante. Purtroppo, questa tecnologia, si è scoperta fragile nella prima versione, perché il pin che viene scambiato tra i due dispositivo è composto da 8 cifre, ma le ultime 4 sono generali dalle prime 4.

Il WPS non è una tecnologia di protezione di una rete, come WEP, WPA/WPA2, ma bensì una tecnologia d'aiuto per collegarsi ad un rete. Per questo motivo, è possibile craccare una rete WiFi utilizzando questo exploit, con uno dei seguenti tool:

- Fern WiFi Cracker
- Reaver
- WPS Pixie (link)

Linee guide per evitare attacchi

Ecco un po' di linee guide, per evitare intrusioni nella propria rete wireless:

- Utilizzare come livello di protezione WPA2
- Cercare di utilizzare una password composta lettere minuscole, maiuscole, numeri, caratteri speciali e abbastanza lunga
- Cercare di cambiare la password durante l'anno
- Disabilitare il WPS
- Effettuare aggiornamenti il più possibile al router
- Evitare di inserire la password del vostro WiFi in pagine WEB

- Evitare di fornire la password della vostra rete ad amici, meglio creare una rete apposta per logo (rete Guest)

Conclusione

Nel mondo della sicurezza informatica, si può tranquillamente sostenere che ottenere accesso ad un qualunque dispositivo, come ad esempio ad una rete WiFi, è questione di tempo e di risorse a disposizione. L'obiettivo degli sviluppatori/ingegneri informatici, è quello di rendere il più lungo possibile tale spazio temporale. Per quanto riguarda le reti WiFi, ci sono diverse tipologie d'attacchi, che funziona a seconda del livello di protezione della rete WiFi e di chi l'amministra. Come già accennato all'inizio, questa guida ha il solo scopo di dare una panoramica riguarda al mondo delle rete WiFi, in modo da potersi adoperare per evitare intrusioni.

Nuovo Raspberry Pi Zero W con modulo WiFi e bluetooth

Dopo il grande successo del Raspberry Pi Zero, la fondazione Inglese rilascia sul mercato un aggiornamento molto interessante, in quanto aggiunge le funzionalità di connessioni senza fili, come WiFi e bluetooth a bordo della scheda.

Ecco la lista completa delle funzionalità del piccolo PC:

- 1GHz, single-core CPU
- 512MB RAM
- Mini-HDMI port
- Micro-USB On-The-Go port
- Micro-USB power
- HAT-compatible 40-pin header
- Composite video and reset headers
- CSI camera connector
- 802.11n wireless LAN
- Bluetooth 4.0

È disponibile anche un nuovo case, dedicato per il piccolo PC, in modo da renderlo trasportabile ovunque in maniera pratica.

Ecco un video panoramica per il nuovo Raspberry Pi Zero W.

Il nuovo Raspberry Pi Zero W è acquistabile da Kubii, con i seguenti kit:

- Raspberry Pi Zero W 11 Euro
- Contenitore Ufficiale Per Pi Zero 5.94 Euro
- Kit Pi Zero W Budget 21,95 Euro
- Kit Pi Zero W Plus 26,90 Euro
- Starter Kit Pi Zero W 31,92 Euro

La pagina dedicata al nuovo prodotto della fondazione, è raggiungibile al seguente link.